UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,882	07/08/2003	Philip Michael Hawkes	030441	9835

23696 7590 12/21/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
12/21/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

Office Action Summary	Application No.	Applicant(s)	
	10/615,882	HAWKES ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-16,19-25,28-34,37-43,46-52 and 55-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-16,19-25,28-34,37-43,46-52 and 55-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 9/19/2007 was received and considered.

2. Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 are pending.

Response to Arguments

3. The amendment to the specification and claims overcomes the objections to the specification and rejections of the claims under 35 U.S.C. §112, as set forth in the previous office action.

4. Applicant's arguments filed 9/19/2007 have been fully considered but they are not persuasive.

5. In response to applicant's argument (specifically, p. 14, ¶3 & p. 17, ¶3) that the examiner has combined an excessive number of references (4 and 3, respectively), reliance on a large number of references in a rejection does not, without more, weigh against the obviousness of the claimed invention. See *In re Gorman*, 933 F.2d 982, 18 USPQ2d 1885 (Fed. Cir. 1991). In the case of cryptography and security, much of the art is a collection of tools such as encryption techniques often combined in various ways to accomplish a task. Such a combination is often based on well known principles or qualities associated with those techniques. Therefore, the examiner maintains that the fact that 3 or 4 references are combined to show various techniques is not a showing of non-obviousness.

6. Applicant's response (pp. 14-15) shows Applicant's interpretation of the examiner's application of the references, specifically alluding to the fact that the application of the references appears inconsistent. In short (for example, claim 1), Lee is cited for disclosing key distribution in a broadcast system. This concept is both old and well known, where keys have different validity periods and are changed through a set of encryptions, where key 1 encrypts key 2, key 2 encrypts key 3 and eventually key N encrypts the data. Wasilewski is cited for teaching the application of asymmetric cryptography in

broadcast distribution. A problem exists in the first distribution system encryption techniques in that key 1 needs to be maintained along with all other key 1's from different subscribers. Wasilewski discloses that a top key in the hierarchy is a private key, which means that the service provider has a public key that it uses. This is useful because it allows the service provider the flexibility to not transfer endless keys because if the public key 1 is "compromised" from the service provider, the key cannot be used to decrypt key 2. This is common knowledge in cryptography and the primary utility of asymmetric cryptography. Tsuria teaches a networking technique that is notoriously well known in the art of computer, security, networking, etc. Tsuria teaches that it is well known to make devices wireless for the purpose of eliminating physical cables, and hence well known to receive data that would normally travel through a communication cable over the air. This technique is ubiquitous. Daly is cited for teaching a video distribution system where the set top box sends it's public key to a headend in the form of a digital certificate. Digital certificates are well known (X.509 is one standard), such that if a user wants to engage another user in asymmetric cryptography, the second user must have the public key that corresponds to the first user's public key. This allows, among other things, the first user to not have a pre-established relationship with the second user. In other words, this allows the first user to choose at any time a second user with whom to communicate securely and to simply give the second user the first user's public key. This concept is also very well known. To address concerns of the wording of the claim rejections, claim 1 is used again as an example. Lee teaches distributing a key corresponding to a key in the terminal, receiving a secret key encrypted by the distributed key, decrypting the secret key with the key in the terminal, receiving an access key at the terminal encrypted by the secret key and decrypting the access key at the terminal with the secret key. Wasilewski teaches motivation for the distributed key to be a public key and the terminal's key to be a private key. Tsuria teaches motivation

for exchanging the keys over the air (wirelessly). Daly teaches motivation for distributing the key over the air from the terminal, since Lee's distribution is silent as to the method. Therefore, for example, Tsuria's "over the air" contribution to the art affects the limitations that contain the phrase "over the air" (limitations 1 and 2 of claim 1).

7. Applicant's response (p. 16, ¶1) again argues the number of references. However, the number of references is alone irrelevant. As described above, because the limitations are taught to be well known and have well known motivation for use in the references, the combination of the well known concepts is maintained as reasonable.

8. Applicant's response (p. 16, ¶1) argues that the examiner's reasons for combining are merely conclusionary. However, as described above and in the rejections themselves, motivation exists in the references and to one having ordinary skill in the art. The example given with Daly is known to one of ordinary skill in the art when reading the reference. Specifically, the passing of the public key allows the subscriber to place an order to interactive programming material.

9. Applicant's response (p. 16, ¶1) argues that the examiner fails to consider the negative aspects of the combinations. However, the combinations neither destroy the references nor render the references' inventions unacceptable for their intended purposes. Applicant gives an example that the "negative aspects of transmitting keys for encryption "over-the-air" are never addressed by the Examiner". However, MPEP 15.04 states that "Once a prima facie case of obviousness has been established, the burden shifts to the applicant to rebut it, if possible, with objective evidence of nonobviousness." Therefore, it is not the responsibility of the office to discuss at length the positives and potential negatives of every possible combination. The burden of non-obviousness shifts to applicant to point out specific errors affecting the assertion of obviousness. However, in the interests of

a complete record, a common "negative aspect" of transmitting a key over the air is the risk of interception by an adversary. However, a public key is just that, public. Hence no negative in the realm of these references exists if the public key is intercepted. Further, the sending of encrypted keys over the air also does not suffer negative consequences of interception because without the private key, the secret key could not be obtained.

10. Applicant's response (p. 16, ¶4) relies on the same impermissible hindsight arguments with respect to claim 1, regarding claims 5, 8, 13-16, 22-25, 31-34, 40-43, 49-52 & 58-61. However, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). As explained above, the knowledge used in combining the references not only appears in the references, but is also well known to those having ordinary skill in the art. Therefore, the rejections are maintained as not relying on impermissible hindsight.

11. Applicant's response (p. 16, ¶5 relating to claim 60) argues that the examiner has not addressed the limitation "user identification module". However, the specification gives no clear description of the metes and bounds of the term "user identification module". Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, since Lee clearly discloses a processor (see Fig. 1's SSTV subscriber receiver), which, as modified, performs the functions set forth in the claim limitations, Lee discloses a processor in a user identification module.

12. Applicant's response (p. 17, ¶2) relies on the same argument with respect to claim 60 above. However, this argument is not persuasive, as described above.

13. Applicant's response (p. 17, ¶3) argues that the examiner is using hindsight. However, as described above, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). As explained above, the knowledge used in combining the references not only appears in the references, but is also well known to those having ordinary skill in the art. Therefore, the rejections are maintained as not relying on impermissible hindsight.

14. Applicant's response (p. 17, last paragraph) incorporates a previous argument into this response. Therefore, the examiner relies on the noted response given previously to this argument (previous office action, p. 3, line 10).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 9-12, 19-21, 28-30, 37-39, 46-48, 55-57 & 62-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Re. 33,189 to Lee et al. (**Lee**) in view of U.S. Patent 5,870,474 to Wasilewski et al. (**Wasilewski**) and U.S. Patent 6,424,947 to Tsuria et al. (**Tsuria**).

Regarding claims 9, 28, 46 & 62, Lee discloses receiving a key (user ID) corresponding to a private key (user ID, col. 3, lines 28-42), encrypting the secret key (key) with the key (user ID, col. 3, lines 42-64), sending the encrypted secret key (key, col. 3, lines 1-22), receiving the access key (random number) at the terminal (subscriber receiver) encrypted by the secret key (key, col. 4, lines 1-22) and decrypting the access key (random number) at the terminal (subscriber receiver) by the secret key (key, col. 3, line 28 - col. 4, line 22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks receiving the public key over the air and sending the encrypted secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a

physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, receive the public key from the terminal (once it is generated, as taught by Wasilewski) over the air and to send the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

Regarding claims 10, 20, 29, 38, 47 & 56, Lee discloses the secret key being a registration key (col. 2, lines 41-51).

Regarding claims 11, 21, 30, 39, 48 & 57, Lee discloses the secret key being a temporary key (key of the month, col. 3, lines 28-42).

Regarding claims 12 & 63, Lee discloses deriving a short key (PN sequence is generated, col. 4, lines 15-18) at the terminal based on the access key (random number), receiving encrypted broadcast content (video) at the terminal and decrypting the encrypted broadcast content at the terminal using the short key (PN sequence, col. 3, line 28 - col. 4, line 22).

Regarding claims 19, 37 & 55, Lee discloses distributing a key (user ID) corresponding to a private key (user ID, col. 3, lines 28-42), receiving a secret key (key, col. 3, lines 42-64) encrypted by the key (user ID, col. 3, lines 42-64), decrypting the secret key (key) by the private key (user ID, col. 4, lines 1-22), encrypting the access key (random number) by the secret key (key, col. 3, lines 42-64) at the content provider (service provider) and sending the encrypted access key (random number, col. 3, line 28 - col. 4, line 22) from the content provider. Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8,

lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit, as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, to receive the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110).

17. Claims 1-5, 8, 13-16, 22-25, 31-34, 40-43, 49-52 & 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Lee** in view of **Wasilewski**, **Tsuria** and U.S. Patent 5,878,141 to Daly et al. (**Daly**).

Regarding claims 1, 22, 40 & 58, Lee discloses distributing a key (user ID, col. 3, lines 28-42), receiving at the terminal (subscriber receiver) a secret key encrypted by the key (user ID, col. 4, lines 1-22), decrypting the secret key (key) with the key (user ID, col. 4, lines 1-22) at the terminal (subscriber receiver), receiving the access key (random number) at the terminal (subscriber receiver) encrypted by the secret key (key, col. 4, lines 1-22) and decrypting the access key (random number) at the terminal (subscriber receiver) by the secret key (key, col. 4, lines 1-22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit, as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the secret key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key

from the terminal (once it is generated, as taught by Wasilewski) over the air and to receive the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110). As modified, Lee lacks distributing the public key over the air from the terminal (STU). However, Daly teaches a video television distribution system (Fig. 3) where the head end server handles both financial transactions and video distribution (col. 9, lines 8-15) that supports two-directional communication (interactive, col. 9, lines 8-15) and where a wireless distribution structure is anticipated (col. 9, lines 35-39). The Daly system purchases data by authenticating the components to the head end system (col. 14, lines 10-18) by exchanging digital certificates between the STB (set top box) and the head end (col. 15, lines 10-26), where the head end can reply using the STB's public key (col. 15, lines 23-26) from the certificate (col. 14, lines 27-32). Since Lee, as modified by Wasilewski, uses a public key of the STU to encrypt the top key in the hierarchy, it would have been obvious to purchase programming by exchanging public keys between the set top unit and the head end and then use the exchanged keys for communication, as taught by Daly. One of ordinary skill in the art would have been motivated to perform such a modification to perform interactive program ordering of services from the head end, as taught by Daly (col. 9, lines 8-15, col. 9, lines 35-39, col. 14, lines 10-32 & col. 15, lines 10-26).

Regarding claims 2, 14, 23, 32, 41, 50 & 59, Lee discloses the secret key being a registration key (col. 2, lines 41-51).

Regarding claims 3, 15, 24, 33, 42 & 51, Lee discloses the secret key being a temporary key (key of the month, col. 3, lines 28-42).

Regarding claim 4, Lee discloses deriving a short key (PN sequence is generated, col. 4, lines 15-18) at the terminal based on the access key (random number), receiving encrypted broadcast content (video) at the terminal and decrypting the encrypted broadcast content at the terminal using the short key (PN sequence, col. 3, line 28 - col. 4, line 22).

Regarding claims 5, 25, 43 & 60, Lee discloses distributing a key (user ID, col. 3, lines 28-42), receiving the broadcast access key/key encrypted by the key (user ID) and decrypting the broadcast access key (key) by the private key (user ID, col. 4, lines 1-22). Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks distributing the public key over the air and receiving the broadcast access key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time

the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key over the air (once it is generated, as taught by Wasilewski) and to receive the broadcast access key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110). As modified, Lee lacks distributing the public key over the air from the terminal (STU). However, Daly teaches a video television distribution system (Fig. 3) where the head end server handles both financial transactions and video distribution (col. 9, lines 8-15) that supports two-directional communication (interactive, col. 9, lines 8-15) and where a wireless distribution structure is anticipated (col. 9, lines 35-39). The Daly system purchases data by authenticating the components to the head end system (col. 14, lines 10-18) by exchanging digital certificates between the STB (set top box) and the head end (col. 15, lines 10-26), where the head end can reply using the STB's public key (col. 15, lines 23-26) from the certificate (col. 14, lines 27-32). Since Lee, as modified by Wasilewski, uses a public key of the STU to encrypt the top key in the hierarchy, it would have been obvious to purchase programming by exchanging public keys between the set top unit and the head end and then use the exchanged keys for communication, as taught by Daly. One of ordinary skill in the art would have been motivated to perform such a modification to perform interactive program ordering of services from the head end, as taught by Daly (col. 9, lines 8-15, col. 9, lines 35-39, col. 14, lines 10-32 & col. 15, lines 10-26). It is noted that the user identification module of Lee is equated to Lee's SSTV subscriber receiver (see Fig. 1) as it includes a processor performing the functions of Lee.

Regarding claims 8 & 61, Lee discloses deriving a short key (random number) at the terminal (col. 4, lines 13-18) based on the access key (key), receiving encrypted broadcast content (video) and

decrypting the encrypted broadcast content (video) using the short key (random number, col. 3, line 28 - col. 4, line 22).

Regarding claims 13, 31 & 49, Lee discloses receiving a key (user ID, col. 3, lines 28-42) at the content provider (service provider), encrypting a secret key (key) using the key (user ID, col. 3, lines 42-64) at the content provider, sending from the content provider the encrypted secret key (key, col. 4, lines 1-5), encrypting the access key (random number) using the secret key (key, col. 3, lines 42-64) at the content provider (service provider) and sending the encrypted access key (random number, col. 4, lines 1-22) from the content provider. Lee lacks a public key. However, Wasilewski teaches that in video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks performing the steps over the air (using a wireless communication structure). However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, to send the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110). As modified, Lee lacks receiving the public key over the air at the content provider (STU). However, Daly teaches a video television distribution system (Fig. 3) where the head end server handles both financial transactions and video distribution (col. 9, lines 8-15) that supports two-directional communication (interactive, col. 9, lines 8-15) and where a wireless distribution structure is anticipated (col. 9, lines 35-39). The Daly system purchases data by authenticating the components to the head end system (col. 14, lines 10-18) by exchanging digital certificates between the STB (set top box) and the head end (col. 15, lines 10-26), where the head end can reply using the STB's public key (col. 15, lines 23-26) from the certificate (col. 14, lines 27-32). Since Lee, as modified by Wasilewski, uses a public key of the STU to encrypt the top key in the hierarchy, it would have been obvious to purchase programming by exchanging public keys between the set top unit and the head end and then use the exchanged keys for communication, as taught by Daly. One of ordinary skill in the art would have been motivated to perform such a modification to perform interactive program ordering of services from the head end, as taught by Daly (col. 9, lines 8-15, col. 9, lines 35-39, col. 14, lines 10-32 & col. 15, lines 10-26).

Regarding claims 16, 34 & 52, Lee discloses receiving a key (user ID, col. 4, lines 1-22) at the content provider (service provider), encrypting the broadcast access key (key) at using the key (user ID, col. 3, lines 42-64) at the content provider and sending the encrypted broadcast access key (key, col. 3, lines 42-64) from the content provider. Lee lacks a public key. However, Wasilewski teaches that in

video distribution, the top key in the hierarchy of keys is a private key stored in a set top unit (col. 8, lines 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41) because using a public key system obviates the need to securely transfer an endless hierarchy of keys (col. 8, lines 34-37) and allows multiple service providers to communicate with the set top unit (col. 10, lines 45-46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top unit) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit as taught by Wasilewski (col. 8, lines 34-47 & col. 10, lines 45-46). As modified, Lee lacks receiving the public key over the air and sending the encrypted broadcast access key over the air. However, Tsuria teaches a system where a wireless subscriber unit receives television transmissions over the air (RF link) (col. 9, lines 35-48) to eliminate the need for a physical cable connection, as shown in Fig. 2 (#106 & #110). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, to send the encrypted broadcast access key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to gain the known benefits of wireless computing devices, such as the elimination of direct cable connections, as taught by Tsuria (col. 9, lines 35-48 & Fig. 2 #106 & #110). As modified, Lee lacks receiving the public key over the air at the content provider. However, Daly teaches a video television distribution system (Fig. 3) where the head end server (content provider) handles both financial transactions and video distribution (col. 9, lines 8-15) that supports two-

directional communication (interactive, col. 9, lines 8-15) and where a wireless distribution structure is anticipated (col. 9, lines 35-39). The Daly system purchases data by authenticating the components to the head end system (col. 14, lines 10-18) by exchanging digital certificates between the STB (set top box) and the head end (col. 15, lines 10-26), where the head end can reply using the STB's public key (col. 15, lines 23-26) from the certificate (col. 14, lines 27-32). Since Lee, as modified by Wasilewski, uses a public key of the STU to encrypt the top key in the hierarchy, it would have been obvious to purchase programming by exchanging public keys between the set top unit and the head end and then use the exchanged keys for communication, as taught by Daly. One of ordinary skill in the art would have been motivated to perform such a modification to perform interactive program ordering of services from the head end, as taught by Daly (col. 9, lines 8-15, col. 9, lines 35-39, col. 14, lines 10-32 & col. 15, lines 10-26).

Commensurate with the method description above, the means for distributing the public key correspond with the set top unit, as modified above, the means for receiving the public key correspond with the headend and then service provider, as modified above, the means for receiving the secret key or broadcast encryption key correspond with the set top unit, as modified above, and the means for sending the secret key or broadcast access key correspond with the headend and service provider.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 12, 2007
Michael J. Simitoski
/Michael J. Simitoski/